North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005

*Indicated a mandatory field

*Name of the Company or Government Agency owning or licensing information affected by the entity experiencing breach:

SANFORD HEISLER SHARP, LLP

Entity Type:	GENERAL BUSINESS
Address:	1350 AVENUE OF THE AMERICAS
Apt/Suite/Building:	31ST FLOOR
City:	NEW YORK
State:	NY
Zip Code:	10019
Telephone:	
Fax:	
Email:	

*Date Security breach Reporting Form Submitted:	07/13/2018
Is this notice a supplement to a previously filed Security Breach:	NO
*Date the Security Breach was discovered:	06/13/2018
Breach Type:	PHISHING
*Estimated number of affected individuals:	413
*Estimated number of NC residents affected:	4

Name of company or government agency maintaining or possessing information that was the subject of the Security Breach, if the agency that experienced the Security Breach is not the same entity as the agency reporting the Security Breach (pursuant to N.C.G.S. 75-65(b))

Describe the circumstances surrounding the Security Breach:	SEE ATTACHED APPENDIX.
Information Type:	ACCOUNT # SSN
*Regarding information breached, if electronic, was the information protected in some manner:	YES
If YES, please describe the	SHS HAD SECURITY MEASURES IN PLACE INCLUDING ANTIVIRUS SOFTWARE, FIREWALLS, PASSWORD PROTECTION, AND OTHER

security measures protecting the information:	SAFEGUARDS RELATED TO SECURING PERSONAL INFORMATION.
*Describe any measures taken to prevent a similar Security Breach from occurring in the future:	TO HELP PREVENT SOMETHING LIKE THIS FROM HAPPENING IN THE FUTURE, SHS IS ENHANCING ITS EXISTING NETWORK SECURITY MEASURES AND PROVIDING TRAINING TO EMPLOYEES ON THE DANGERS OF PHISHING EMAILS.
*Date affected NC residents were/will be notified:	07/13/2018
Describe the circumstances surrounding the delay in notifying affected NC residents pursuant to N.C.G.S. 75-65 (a) and (c):	NOTICE IS BEING PROVIDED WITHOUT DELAY.

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. 75-65(c), please attach or mail the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. 75-65 (e)):

WRITTEN NOTICE

Please note if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2) , or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

- Email notice when the business has an electronic mail address for the subject persons
- Conspicuous posting of the notice on the Web site page of the business, if one is maintained
- Notification to major statewide media

Please attach a copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

Contact Information Affiliation with entity experiencing breach:	ATTORNEY

Organization Name:	BAKER & HOSTETLER LLP		
Prefix:	MR		
*First Name:	DAVID		
Middle Name:			
*Last Name:	KITCHE		
Suffix:			
Title:	PARTNER		
Address:	KEY TOWER, 127 PUBLIC SQUARE		
Apt/Suite/building:	SUITE 2000		
City:	CLEVELAND		
State:	OH	Zip Code:	44114
*Telephone:	(216) 621-0200	Fax:	
Email:	DKITCHEN@BAKERLAW.COM		

North Carolina Appendix

On May 23, 2018, Sanford Heisler Sharp, LLP ("SHS"), learned through its ongoing forensic investigation into a phishing incident that an unauthorized party obtained access to an email account belonging to an SHS partner. Upon learning of the phishing incident, SHS immediately reset passwords for all affected employee accounts and began an investigation with the assistance of a professional forensic firm. The investigation determined that unauthorized individual(s) had accessed the partner's account from May 9, 2018 through May 14, 2018. The investigation was unable to determine the scope of information that may have been viewed or acquired by the individual(s). Therefore, SHS provided notice to all individuals whose information was contained in the email account. On June 13, 2018, SHS learned that the email account may contain information pertaining to North Carolina residents. For each of the North Carolina residents, the emails and attachments contained the individual's name and one or more of the following data elements: Social Security number, and financial account number.

On July 13, 2018, SHS will begin mailing written notifications to potentially affected individuals, including four (4) North Carolina residents who are being notified of the incident in writing in accordance with N.C.G.S. 75-65 in substantially the same form as the enclosed letters. SHS is offering all eligible potentially affected individuals a complimentary one-year membership in credit monitoring and identity theft protection services from Experian's® IdentityWorksSM Credit 3B. SHS is also providing a telephone number for potentially affected individuals to call with any questions they may have.

To help prevent something like this from happening in the future, SHS is enhancing its existing network security measures and providing training to employees on the dangers of phishing emails.

This report is not, and does not constitute, a waiver of SHS's objection that North Carolina lacks personal jurisdiction regarding the company related to this matter.

c/o RG/2 Claims Administration
P.O. Box 59479
Philadelphia, PA 19103-9479

July 13, 2018

<Name>
<Address>
<City>, <State> <Zip code>
<country>

NOTICE OF DATA BREACH

Dear <Name>:

Sanford Heisler Sharp, LLP ("SHS") understands the importance of protecting personal information entrusted to us. We are writing to inform you that we recently identified and addressed a security incident that may have involved your personal information. This notice explains the incident, measures we have taken, and some steps you can take in response.

What Happened: On May 23, 2018, we learned through our ongoing forensic investigation into a phishing incident, that an unauthorized party obtained access to an email account belonging to an SHS partner. Upon first learning of the phishing incident, we immediately reset employee passwords and began an internal investigation. We also engaged a leading cyber security firm to perform an investigation to determine what, if any, sensitive information may have been accessed. The investigation determined that unauthorized individual(s) had accessed the partner's account. The investigation was unable to determine the scope of information that may have been viewed or acquired by the individual(s). We are therefore providing you this notice so that you understand the nature of your information and can take steps to help protect yourself.

What Information Was Involved: The emails and attachments contained in the partner's account include your name<variable data>.

What You Can Do: We encourage you to remain vigilant by reviewing your account statements for any unauthorized activity. You should also review the additional information on the following pages on ways to protect yourself**. In an abundance of caution, we have arranged for you to receive a complimentary one-year membership of Experian's® IdentityWorks℠ Credit 3B**. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

What We Are Doing: We apologize for any inconvenience caused by this incident. To help prevent this type of incident from happening again, we are taking steps to enhance our existing network security measures and providing training to employees on the dangers of phishing emails.

For More Information: If you have questions about this incident or the recommended next steps, please call 866-742-4955, Monday through Friday between 9:00 am and 5:00 pm Eastern Time.

Sincerely,

Jeremy Heisler
Vice Chairman

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **October 31, 2018** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332. Be prepared to provide engagement numbe[redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-890-9332 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-890-9332.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

Even if you choose not to take advantage of this complimentary credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center**,** 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

You may contact and obtain information from the Connecticut Attorney General's Office at:

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

You may contact and obtain information from the Maryland Attorney General's Office at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland) or 1-410-576-6300 (for calls originating outside Maryland)

You may contact and obtain information from the North Carolina Attorney General's Office at:

North Carolina Attorney General, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or toll free at 1-877-566-7226

There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit

report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

c/o RG/2 Claims Administration
P.O. Box 59479
Philadelphia, PA 19102-9479

July 13, 2018

<Name>
<Address>
<City>, <State> <Zip code>
<country>

NOTICE OF DATA BREACH

Dear <Name>:

Sanford Heisler Sharp, LLP ("SHS") understands the importance of protecting personal information entrusted to us. We are writing to inform you that we recently identified and addressed a security incident that may have involved your personal information. This notice explains the incident, measures we have taken, and some steps you can take in response.

What Happened: On May 23, 2018, we learned through our ongoing forensic investigation into a phishing incident, that an unauthorized party obtained access to an email account belonging to an SHS partner. Upon first learning of the phishing incident, we immediately reset employee passwords and began an internal investigation. We also engaged a leading cyber security firm to perform an investigation to determine what, if any, sensitive information may have been accessed. The investigation determined that unauthorized individual(s) had accessed the partner's account. The investigation was unable to determine the scope of information that may have been viewed or acquired by the individual(s). We are therefore providing you this notice so that you understand the nature of your information and can take steps to help protect yourself.

What Information Was Involved: The emails and attachments contained in the partner's account include your name<variable data>.

What You Can Do: We encourage you to remain to vigilant to the possibility of fraud by reviewing your financial statements and credit reports for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported. You should also review the additional information on the following page on ways to protect yourself.

What We Are Doing: We apologize for any inconvenience caused by this incident. To help prevent this type of incident from happening again, we are taking steps to enhance our existing network security measures and providing training to employees on the dangers of phishing emails.

For More Information: If you have questions about this incident or the recommended next steps, please call 866-742-4955, Monday through Friday between 9:00 am and 5:00 pm Eastern Time.

Sincerely,

Jeremy Heisler
Vice Chairman

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center**,** 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

You may contact and obtain information from the Connecticut Attorney General's Office at:

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

You may contact and obtain information from the Maryland Attorney General's Office at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland) or 1-410-576-6300 (for calls originating outside Maryland)

You may contact and obtain information from the North Carolina Attorney General's Office at:

North Carolina Attorney General, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or toll free at 1-877-566-7226

There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit

freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.